(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 January 2001 (04.01.2001)

PCT

(10) International Publication Number
WO 01/01629 A1

(51) International Patent Classification[7]: H04L 9/32, 9/30

(21) International Application Number: PCT/EP00/05642

(22) International Filing Date: 19 June 2000 (19.06.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1012435 25 June 1999 (25.06.1999) NL

(71) Applicant *(for all designated States except US)*: KONINKLIJKE KPN N.V. [NL/NL]; Stationsplein 7, NL-9726 AE Groningen (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: DE BOER, Marten [NL/NL]; Egypte 2, NL-9285 WX Buitenpost (NL). KLEINHUIS, Geert [NL/NL]; Mindertfaen 1, NL-9264 TX Eernwoude (NL).

(74) Agent: KLEIN, Bart; Koninklijke KPN N.V., P.O. Box 95321, NL-2509 CH The Hague (NL).

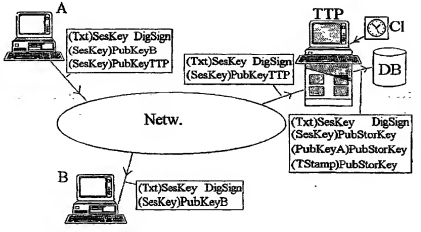
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM FOR PROTECTED STORAGE AND MANAGEMENT IN A TTP SERVER



(57) Abstract: System for protected storage in a TTP server. A file (Txt) is transmitted from a first (A) to a second user (B) after being enciphered with a session key (SesKey), which is enciphered with the public key (PublKeyB) of the second user. The session key (SesKey) is also enciphered by the first user with the public key (PublKey/TTP) of the TTP server which, after having received it, deciphers said session key with his private key (SecKeyTTP). The TTP server subsequently enciphers the session key (SesKey) and the (original) public key (PubKeyA) of the first user (A) with a "public" storage key (PubStorKey). The enciphered session key ((SesKey)PubStorKey) and public key ((PubKeyA)PubStorKey) of the first user are stored, together with the enciphered file ((Txt)SesKey), in a storage medium (DB). They are recoverable by the TTP, by deciphering with the private storage key (SecStorKey), and may be transmitted after having been enciphered with the current public keys (PubKeyA' or PubKeyB', as the case may be) of the users.

WO 01/01629 A1